

A Novel Approach to privacy-preserving of IoT Devices

Abhinav Divvela, Dr. PVRD Prasad Rao KLEF University

Abstract: In today's everlasting technological world, information and data communication create more devices stay connected to the internet. This lead to achieving development for building different software and internet connection very inexpensive this affected privacy and security. Security today became of the most important issue because day-by-day new technologies are put forward for different purposes of study while these come with a lot of vulnerabilities which makes the exploitation of the data. IoT is also such kind technology which is available for exploiting. For preserving information from such type of attacks here are how blockchain is used to preserve the privacy of IoT devices from being attacked and maintain an open-access Distributed cloud for IoT Devices.

Introduction: With the rapid growth of data processing and information technology in past few decades one of the biggest innovation in this century is Internet of Things termed as IoT which the combination of two words i.e Internet and physical things or objects is i.e. where each physical object is connected to the internet using the RFID tags, sensors, actuators etc. which allows transferring information between the computing devices without the intervention of mankind. The rapid growth of the internet has been increased during this century which enabled the growth of internet of things a lot which is connected through a network with a wired or wireless technology. In-depth research for the origination of IoT in the late 1960's communication between the two computing devices is done through the computer network. Later in the early 80's TCP/IP was introduced which led the invention of WWW in early 90's which made internet more circulation with a rapid growth for people and Internet of Things started increasing from late 90's. The term IoT is originated by Kevin Ashton, executive director of the AutoID center in Massachusetts Institute of Technology (MIT) in the year 1999.

As an enormous growth of internet helped the growth of IoT applications in various fields which induced into human day-to-day life. As IoT applications are build using internet security became an important obstruct for IoT applications where data from the user/organization is breached and been vulnerable to malicious attacks performed by the attacker. There

are several attacks that can be performed to make IoT system more vulnerable such as Man-In-The-Middle (MITM), Sniffing, Denial of Service (DoS), Cryptographical attacks, Botnet attacks, Denial of Service (Dos) and Distributed Denial of Service (DDoS). This paper mainly deals when an IoT device is been attacked by above attacks and in order to control such type of attacks this paper also provides a solution on IoT system/network/application by introducing blockchain technology which handles better security for IoT.

The initial work on a cryptographically secured chain of blocks was outlined in 1991 by Stuart Haber and W. Scott Stornetta with a design of Merkle trees, which improved efficiency by providing various documents to be stored into a single block. A blockchain is decentralized and distributed digital ledger for cryptocurrency and stores a list of transactions from many computers such that past records cannot be changed without changing of succeeding blocks and collusion of the network. This provides various participants to verify and examine transactions without central recordkeeping. The blockchain database is shared by all nodes participating in a system where each node gets a copy of the chain and can be downloaded automatically using peer-to-peer connections. Each block contains a hash of the preceding block and computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. The blockchain is a main innovation of bitcoin. The blockchain based exchange of value can be completed more rapid, with a low cost and provides high protection with respect to traditional systems. In August 2008 Satoshi Nakamoto linked a paper Peer-to-peer Electronic Cash System which described as a system that transmits electronic transactions without trust and in the later year, January 2009 first open source Bitcoin client was initialized. In the year 2013 bitcoin fraudulent has been found after a hacker illegally transferred a large number of bitcoins from Mt. Gox auditor by compromising the computer. After two years of vivid research, thus researchers found blockchain technology for protecting and privacy of bitcoins, digital currency, IoT and a lot more things that can be done using Blockchain.

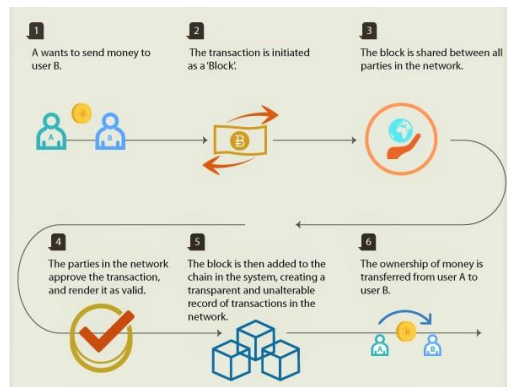


Fig 1: Block chain working

Literature Survey: [13] Nir Kshetri provides an information on securing Internet of Things(IoT) using a blockchain protecting and privacy technologies where some specific measures are needed to be taken care at various levels to integrate blockchain in IoT and it provides an information based on user identity and access management systems using a centralized and decentralized blockchain cloud model in IoT.[1] Seyoung Huh, Sangrae Cho, and Soohyung Kim provided information on Managing IoT Devices Using Ethereum concept where a user sets the network configuration via a smartphone network thus concurrently executing three different processes and this also builds IoT system to withstand against many denial of service and forgery attacks.[2] Ali Dorri, Salil S.Kanhere, Raja Jurdak and Praveen Gauravaram illustrated a local ledger of the BC and also implemented the blockchain technology in smart home which involves transaction handling, storing of transaction with evaluation of packet overhead, time overhead and energy consumption with other peoples and also provides an overlay of different types of attacks that are been performed during the analysis.[3] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park and Kyung-Hyune Rhee illustrated the implementation of blockchain in different applications rather than in the field of technology.

Types of Attacks:

A port scan is a passive attack where it can't harm any system or server, but it is a simple probe which retrieves the complete details of victim machine or servers and vulnerabilities to the attacker. Port scan is a procedure that sends requests to a client that are in a

range of server port addresses on a host with an aim of finding any active port. There are different types of port scans among them TCP Connect, SYN scan, UDP scan, XMAS scan, ACK scan and FIN scan are most scans used by an attacker.

Man-In-The-Middle also known as MITM attack is a typical type of attack in which attacker tries to intercept communication between two parties. In other words, we can say this attack as a Janus attack (or) active eavesdropping because the attacker frames a reliable connection between the two parties and relays messages on either side such that to make a belief they are in a private conversation, but the entire communication is managed by the attacker.

Denial of Service attack is one of a type of attack which is used to shut down machine (or) network (or) application for a period such that it user can't use the system/network. It is done through pingging the network/system with heavy spam requests such that system/network can't able to handle those many requests which will lead the system to crash because it has a limited capability. Mostly attacker tries to attack using botnet and buffer overflow vulnerability and common victims of this attacks are high profile organizations like banking and government sectors which lead them the loss of important data and time to fix back the system/network.

Distributed Denial of Service attack is like Denial of service attack but here attacker doesn't involve directly rather than he uses several systems to take down the machine/network such that it causes a temporary denial of service for users in the organization. A typical DDoS attack consists of master and zombie where master is referred to the attacker who initially start the attack by exploiting a vulnerability in the system and identifies other vulnerable systems and attain command over them either by infecting systems through malware or bypassing the general authentication access which are used commonly while the zombie is the list of systems or network components that are under the control of master. It is also called as Bot.

Sniffing attack is a common type of attack that can be performed over the wired and wireless networks which will help the attacker to get access over the device such that attacker can obtain, collect and modify information from the device (or) machine. The main purpose of using sniffing attack is to obtain access over a network and then later attacker access

the internet without any restriction. There are two most important methods that are used by the attacker during sniffing that includes ARP poisoning and TCP session stealing methods. ARP poisoning is a method in sniffing attack where it is used to attack the network with packet-spoofing attacks and router-based vulnerabilities while TCP session stealing method is used to catch the source and destination IP address packets in promiscuous mode.

The most common widely used and successful Cryptographical attacks are Social engineering for key discovery, Dictionary attack, Reverse engineering, Brute-force attack and Implementation attacks where social engineering for key discovery depends upon humans to implement and operate the intellectual property illegal while dictionary attack is used for retrieving password files when the user chooses a common detectable password by using simple and natural words. There is a software which encrypts all the words in the dictionary and checks the hash result that matches the encrypted password which is stored in the password file. Implementation attacks are also called as the algorithmic attack because these are implemented by the elements outside the system. There are three main implementation types of attacks which comprise of side-channel attack, probing attack and fault analysis.

Proposed model:

An appealing methodology for answering the issue of the high computational power that is required so as to communicate with the Blockchain technology is to organize an incorporated decentralized combined architecture i.e to establish intermediate servers between IoT device and the Blockchain. Privacy control confronts enormous difficulties in IoT. Unluckily, it is difficult to execute current privacy control norms on small things because of its coerce nature while the presentation of effective and trusted a third party to deal with privacy control rationale could harm clients security. In this work, we demonstrate how blockchain technology, the promising innovation behind Bitcoin, can be fascinating to confront those emerging challenges. We along these lines propose FairAccess as another decentralized pseudonymous what's more, security safeguarding approval administration structure that influences the consistency of blockchain technology to manage privacy control on constrained IoT devices.

The implementation of IoT devices which relate to the connectivity problems of open access IoT networks which are in today has several concerns regarding the security, cost, and privacy of the Internet of Things where most of them are connected to the Centralized cloud with a single connection. The below diagram shows how different things are connected to a centralized cloud through an internet connection. Due to this if any security issues arise all the IoT devices that are connected can be disconnected this may lead to the data breach and privacy of the user. When all the devices stop working without the connection to the internet most of the IoT devices are useless and it makes a heavy burden for the user to replace the devices which cost him a lot.



Fig 2: Centralized Cloud Connected IoT Device

But when a blockchain technology is implemented to the Internet of things that are inter-connected without centralized cloud internet connection they are connected to blocks of things which are interlinked with blocks of the internet. Thus, it reduces the centralized cloud connectivity by decentralizing and protects with highly secure connectivity with the user privacy which integrates all things/devices with a single authentication and eliminates counterfeits. The future of the Internet of things will mainly depend on the blockchains with an open Registry for each device that is connected to the internet. There are

some more important aspects when we implement blockchain on the Internet of Things (IoT) devices which reduce infrastructure cost and increases smart contracts which are used to buy, sell, rent and lease devices readily without any delay.

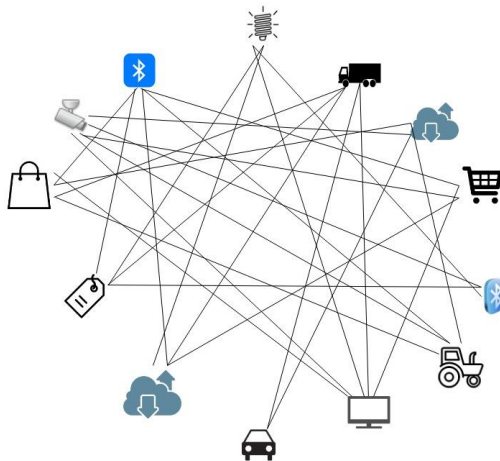


Fig 3: Implementation of blockchain in IoT device

Future Work and Conclusion:

The main objective of this work is to make the possibility of using blockchain technology in the field of security in the Internet of Things. IoT security is acquiring a great attentiveness nowadays from both scholarly communities and in industry. Existing security measures are not really suited for IoT because of high energy utilization and preparing overhead. For this purpose, we implemented blockchain in IoT. Apart from the field of technology blockchain can be implemented in different fields such as commodities, healthcare, digital identity & authentication, gaming & gambling, network infrastructure, real estate, social networks and in supply chain certification in the food industry.

References

- [1] Seyoung Huh, Sangrae Cho and Soohyung Kim "Managing IoT devices using Blockchain Platform" in *International conference in Advanced Communication Technology (ICACT)*, in Feb. 2017
- [2] Ali Dorri, Salil S.Kanhere, Raja Jurdak and Praveen Gauravaram "Blockchain for IoT security and privacy: The case study of a smart home" in *IEEE International Conference on Pervasive Computing and Communications Workshops* in May 2017
- [3] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park and Kyung-Hyune Rhee "A critical review of blockchain and its current applications" in *International Conference on Electrical Engineering and Computer Science (ICECOS)* in Dec.2017
- [4] Yu Zhang, Jiangtao Wen "The IoT electric business model: Using blockchain technology for the internet of things" in *Peer-to-peer Networking and Applications*, volume 10, Issue 4, pp 983-994, Apr.2016
- [5] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gun Sirer, Dawn Song, and Roger Wattenhofer, "On Scaling Decentralized Blockchains", *Initiative for CryptoCurrencies and Contracts (IC3)*, 2016
- [6] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [7] Konstantinos Christidis and Micheal Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", *IEEE Access* (Volume: 4), 2016.
- [8] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *2016 IEEE European Symposium on Security and Privacy (EuroSP)*, 2016, pp. 305–320.
- [9] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016*. Springer Berlin Heidelberg, 2017, pp. 515–532.
- [10] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive Compatibility of Bitcoin Mining Pool Reward Functions". *Springer Berlin Heidelberg*, 2017, pp. 477–498.
- [11] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, ser. EC '16. ACM, 2016, pp. 365–382.
- [12] J. Herrera-Joancomartí and C. P'erez-Sol'a, "Privacy in bitcoin transactions: New challenges from blockchain scalability solutions," in *Modeling Decisions for Artificial Intelligence: 13th International Conference, MDAI 2016*. Springer International Publishing, 2016, pp. 26–44.
- [13] Nir Kshetri "Blockchain's roles in strengthening cybersecurity and protecting Privacy" in *Telecommunications Policy of ScienceDirect*, Vol 41, Pages 1027-1038, Nov.2017

